

FUNCTION FIELDS OF CLASS NUMBER ONE

QIBIN SHEN AND SHUHUI SHI

ABSTRACT. In 1975, J. Leitzel, M. Madan and C. Queen listed 7 function fields over finite fields (up to isomorphism) with positive genus and class number one. They claimed to prove that these were the only ones such. Recently, Claudio Stirpe found an 8th one! In this paper, we fix the argument in the former paper to show that this 8th example could have been found by their method and is the only one, so that the list is now complete.

1. INTRODUCTION

It is not yet known whether there are infinitely many number fields of class number one (let alone, real quadratic number fields of class number one, as Gauss conjectured). The classification of imaginary quadratic fields was completed by Heegner and Stark only in 1969, but it was only in 1983 through the works [G85] of Goldfeld and Gross-Zagier that it was established that the imaginary quadratic fields of given class number can be effectively classified.

In the case of (global) function fields (i.e., function fields over finite fields \mathbb{F}_q), there are no archimedean places at ‘infinity’, so there is no canonical ring of integers and its class group. In fact, there are several variants of class groups, see e.g., [T04, Chapter. 1] for more detailed discussion and references. The usual substitute, which we will use below, is the divisor class group of degree zero (or what is the same, the group of \mathbb{F}_q -rational points of the corresponding Jacobian).

All the genus zero function fields, namely the rational function fields $\mathbb{F}_q(t)$, one for each q , have class number one. MacRae [M71] classified class number one ‘imaginary quadratic fields’. Also, we can, in fact, effectively determine all function fields of a given class number (even when q or the characteristic is not fixed), and we will quickly recall this below for the benefit of the reader. But even today, with the powerful computers, it is not so easy to do this even for class number one.

In M. Madan and C. Queen’s paper [MQ72], it was shown that except for a possible exception of genus 4 function field with field of constants \mathbb{F}_2 , there are only 7 class number one function fields of positive genus. Then J. Leitzel, M. Madan and C. Queen claimed to finish the classification in [LMQ75] by showing such exception does not exist. (A somewhat similar history to Heegner-Stark’s proof of the non-existence of the last possible exception known since 1934!). But this was a mistake: recently Claudio Stirpe [S14] found an explicit 8th example, of the type ruled out.

As [S14] left the question open whether the example was the only counter-example, we went through the arguments of [LMQ75] and found exactly one more counter-example, the one given by Stirpe. After informing Stirpe of this, we were told by him that, jointly with Mercuri, he also had recently succeeded in proving the same result. The preprint [MSP14] has now appeared. We are submitting our

independent work, cutting out unnecessary duplication with the work of Mercuri and Stirpe. It should be noted that [MSp14] offers two proofs, the second being essentially the same as ours.

2. CLASSIFYING FUNCTION FIELDS OF A GIVEN CLASS NUMBER

Let us recall some basic facts of the theory of global function fields (see e.g., [T04, Chapter 1] for references) for the benefit of the reader.

Let K be a function field with field of constants \mathbb{F}_q , of genus $g > 0$, class number h and zeta function $Z(t)$.

It is well-known through the works of Artin, Hasse and Weil that the class number h is equal to $P(1)$, where $P(t) = \prod_{i=1}^{2g} (t - \alpha_i)$ is the numerator of the zeta function. By Weil's theorem, which is the analog of Riemann hypothesis, the α_i 's have absolute value \sqrt{q} . Hence

$$h \geq (\sqrt{q} - 1)^{2g}.$$

It follows that $h > 1$ if $q > 4$, and more generally, an upper bound on h implies an upper bound on g .

Let N_i be the number of \mathbb{F}_{q^i} -rational points of the projective non-singular curve corresponding to K , and let N denote the number of degree one primes for the constant field extension of degree $2g - 1$ of K . Then an easy argument ([MQ72, p. 424], modified in a straight-forward way from the $h = 1$ case there) implies that

$$h(2g - 1)(q^g - 1)/(q - 1) \geq N \geq q^{2g-1} + 1 - 2gq^{(2g-1)/2},$$

where the first inequality holds by Riemann-Roch theorem and the second is by the Weil bound. (If one is only interested in an effective algorithm to classify function fields of a given class number, then one can use weaker easily proved bounds instead of the Weil bounds). Hence the upper bound on h implies an upper bound on g and q . But there are only finitely many function fields of given g and q and they can be effectively determined (see e.g., [T04, p. 12] and references there). Thus there is an effective (but quite unpractical) algorithm to classify function fields with given h .

The bound above implies [MQ72, Thm. 1] that if $h = 1$, then $g = 1$ for $q = 4$, $g \leq 2$ for $q = 3$ and $g \leq 4$ for $q = 2$. A more sophisticated argument allows classification except for the $g = 4$, $q = 2$ case (where $h = 1$ implies $N_1 = N_2 = N_3 = 0$ and $N_4 = 1$).

3. FIXING THE ARGUMENTS IN [LMQ75]

The method of [LMQ75] is correct and does, in fact, show that there is a unique class number one example of genus 4 over \mathbb{F}_2 . But in checking all the possible candidate cases, they had discarded wrongly the unique correct case, as we found out and as also pointed out in [MSp14]. To avoid the duplication, we refer to the end of [MSp14] for details and notation, and content ourselves with only a few relevant comments.

In the end of [MSp14], the authors gave a table of rational points of curves defined by C_i and $Q_i + L(k_1, k_2, k_3, k_4)^2$, $i = 1, 2, 3, 4$, where

$$\begin{aligned}
C_1 &= x_2^3 + x_1x_3^2 + x_4^3 + x_1^2x_3 + x_3x_4^2, \\
Q_1 &= x_1x_2 + x_3x_4, \\
C_2 &= x_2^3 + x_1x_3^2 + x_2^2x_3 + x_2^2x_4 + x_1^3 + x_3^2x_4 + x_1^2x_2 + x_2x_4^2, \\
Q_2 &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_4, \\
C_3 &= x_2^2x_3 + x_1x_4^2 + x_3^3 + x_3^2x_4 + x_1^2x_2 + x_4^3 + x_1^2x_3 + x_3x_4^2, \\
Q_3 &= x_1x_3 + x_2x_3 + x_2x_4 + x_3x_4, \\
C_4 &= x_1^3 + x_1^2x_3 + x_1x_4^2 + x_2^2x_4 + x_2x_4^2 + x_3^3 + x_3x_4^2 + x_4^3, \\
Q_4 &= x_1x_4 + x_2x_3 + x_3x_4, \\
L(k_1, k_2, k_3, k_4) &= k_1x_1 + k_2x_2 + k_3x_3 + k_4x_4, \quad k_i \in \mathbb{F}_2.
\end{aligned}$$

In fact, one only needs to check 24 possible cases among the 64 pairs listed there. This is because for each i , $Q_i + L(k_1, k_2, k_3, k_4)^2$ is equivalent to $X_1X_2 + X_3X_4 + X_3^2 + X_4^2$, as explained in [LMQ75]. This restriction reduces the sixteen $L(k_1, k_2, k_3, k_4)$'s to six for each Q_i . They are:

$$\begin{aligned}
Q_1 &: L(0, 0, 1, 1), L(0, 1, 1, 1), L(1, 0, 1, 1), L(1, 1, 0, 0), L(1, 1, 0, 1), L(1, 1, 1, 0), \\
Q_2 &: L(0, 0, 1, 0), L(0, 1, 0, 1), L(1, 0, 1, 1), L(1, 1, 0, 1), L(1, 1, 1, 0), L(1, 1, 1, 1), \\
Q_3 &: L(0, 1, 0, 1), L(0, 1, 1, 1), L(1, 0, 0, 0), L(1, 0, 1, 1), L(1, 1, 1, 0), L(1, 1, 1, 1), \\
Q_4 &: L(0, 1, 1, 0), L(0, 1, 1, 1), L(1, 0, 0, 1), L(1, 0, 1, 1), L(1, 1, 0, 0), L(1, 1, 1, 1).
\end{aligned}$$

We checked these twenty-four $L(k_1, k_2, k_3, k_4)$'s using SAGE and found that all but one of the candidate fields have points of degree less than or equal to 3. The only exception, $Q_2 + L(1, 0, 1, 1)^2$, gives the unique 8th function field of genus 4 and class number 1. By uniqueness, it has to be isomorphic to Stirpe's counter-example, but (given the history!) we double checked the exact isomorphisms using MAGMA to find it and then checking again by SAGE.

Remarks:

- (1) A minor simplification of [LMQ75] is that the discussion [LMQ75, p. 14] of the cubic forms uniquely decomposing into linear combinations of "special" cubics and multiples of non-degenerate F_2 is not necessary. Any F_3 the W_i 's satisfy which is not a multiple of F_2 works. And the F_3 the paper found from F_2 works, since otherwise it should contain terms like $W_iW_jW_k$ with i, j, k distinct.
- (2) In the start of the proof, the zeta function is stated incorrectly in [LMQ75, p. 12] by missing term $2U^2$, but this has no consequence, and is just a misprint [MQ72, p. 430].
- (3) Dinesh Thakur suggested that we should point out that Stirpe's example should be added to exception list of [T04, Thm. 8.3.1] and [T93, Thm. 3.2], which relied on [LMQ75].

Acknowledgments We thank our advisor Dinesh Thakur for suggesting this problem and for his advice. We thank David Goss for his encouragement, and the referee and Brendan Murphy for suggestions on improving the write-up.

REFERENCES

- [G85] D. Goldfeld, *Gauss's class number problem for imaginary quadratic fields*, Bull. Amer. Math. Soc. 13 (1985), no. 1, 23-37.
- [M71] R. E. MacRae, *On unique factorization in certain rings of algebraic functions*, J. Algebra 17, (1971), 243-261.
- [MQ72] M. L. Madan, C. S. Queen, *Algebraic function fields of class number one*, Acta Arith. XX(1972), 423-432.
- [LMQ75] J. R. C. Leitzel, M. L. Madan, C. S. Queen, *Algebraic function fields with small class number*, J. Number Theory 7, 11-27 (1975)
- [MSp14] P. Mercuri, C. Stirpe, *Classification of Algebraic Function Fields with Class Number One*, arXiv:1406.5365v3, December 2 (2014).
- [S14] C. Stirpe, *A counterexample to 'Algebraic function fields with small class number'*, J. Number Theory 143 (2014), 402-404.
- [T93] D. S. Thakur, *Shtukas and Jacobi sums*, Inventiones Math. 111 (1993), no. 3, 557-570.
- [T04] D. S. Thakur, *Function Field Arithmetic*, World Sci., NJ, 2004.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ROCHESTER, ROCHESTER, NY 14627 USA,
 QSHEN4@UR.ROCHESTER.EDU, SSHI10@UR.ROCHESTER.EDU